

## WHAT IS CLAIMED

1           1.     A kernel-level transaction system, comprising:  
2           plural kernel objects to implement a transaction having plural operations;  
3     and  
4           a security descriptor, applied to at least one of the kernel objects, to identify  
5     at least one user, to identify one of the operations of the transaction that may be  
6     performed on the kernel object to which the security descriptor is applied, and to identify  
7     a right indicating that the identified user is permitted or prohibited to perform the  
8     operation.

1           2.     A system according to Claim 1, wherein the plural kernel objects  
2     include:  
3           a transaction object to represent a transaction;  
4           a resource manager object to represent a resource participating in the  
5     transaction; and  
6           an enlistment object to enlist participants in the transaction.

1           3.     A system according to Claim 1, wherein the security descriptor  
2     comprises at least one access control entry (ACE), which includes a security identifier  
3     (SID) and rights corresponding to the SID.

1           4.     A system according to Claim 2, wherein the security descriptor is  
2 applied to the transaction object, and the operation identified by the security descriptor  
3 includes at least one of:

4                 set information regarding the transaction object,  
5                 enlist the transaction object in the transaction,  
6                 render data updates in connection with the transaction object durable,  
7                 abort the operation on the transaction object,  
8                 transmit data from the transaction object to another object,  
9                 save the current point of the transaction at the transaction object, and  
10                transmit data regarding the transaction to another device.

1           5.     A system according to Claim 2, wherein the security descriptor is  
2 applied to the resource manager object, and the operation identified by the security  
3 descriptor includes at least one of:

4                 retrieve information regarding the resource manager object,  
5                 set information regarding the resource manager object,  
6                 determine the state of a transaction at a moment of transaction failure,  
7                 enlist the resource manager object in a transaction,  
8                 register the resource manager object in the transaction,  
9                 receive notification upon resolution of a transaction at the resource manager  
10                object, and  
11                set resource data in accordance with the transaction resolution.

1           6.     A system according to Claim 2, wherein the security descriptor is  
2 applied to the enlistment object, and the operation identified by the security descriptor  
3 includes at least one of:

4                 get information regarding the enlistment object,  
5                 set information regarding the enlistment object,  
6                 determine a state of enlistments at a moment of transaction failure  
7                 obtain and reference an enlistment key,  
8                 rollback the transaction and to respond to notifications, and  
9                 perform operations a superior transaction manager would perform.

1           7.     A method of implementing a kernel-level transaction, comprising:  
2                 attaching a security descriptor to at least one of plural kernel objects  
3 utilized in a transaction; and  
4                 performing an operation for a transaction on the at least one kernel object in  
5 accordance with the rights accorded by the security descriptor attached to the at least one  
6 kernel object.

1           8.     A method according to Claim 7, wherein the security descriptor  
2 includes identification for at least one user, an operation that is able to be performed on  
3 the at least one kernel object to which the security descriptor is attached, and a right  
4 indicating that the identified user is permitted or prohibited to perform the operation.

1                   9.     A method according to Claim 8, wherein the at least one kernel  
2     object is a transaction object.

1                   10.    A method according to Claim 8, wherein the at least one kernel  
2     object is a resource manager object.

1                   11.    A method according to Claim 8, wherein the at least one kernel  
2     object is an enlistment object.

1                   12.    A method according to Claim 9, wherein the operation identified by  
2     the security descriptor attached to the transaction object includes at least one of:  
3                   set information regarding the transaction object,  
4                   enlist the transaction object in the transaction,  
5                   render data updates in connection with the transaction object durable,  
6                   abort the operation on the transaction object,  
7                   transmit data from the transaction object to another object,  
8                   save the current point of the transaction at the transaction object, and  
9                   transmit data regarding the transaction to another device.

1                   13.    A method according to Claim 10, wherein the operation identified by  
2     the security descriptor attached to the resource manager object includes at least one of:  
3                   retrieve information regarding the resource manager object,  
4                   set information regarding the resource manager object,  
5                   determine the state of a transaction at a moment of transaction failure,

6 enlist the resource manager object in a transaction,  
7 register the resource manager object in the transaction,  
8 receive notification upon resolution of a transaction at the resource manager  
9 object, and  
10 set resource data in accordance with the transaction resolution.

1 14. A method according to Claim 11, wherein the operation identified by  
2 the security descriptor includes at least one of:  
3 get information regarding the enlistment object,  
4 set information regarding the enlistment object,  
5 determine a state of enlistments at a moment of transaction failure,  
6 obtain and reference an enlistment key,  
7 rollback the transaction and to respond to notifications, and  
8 perform operations a superior transaction manager would perform.

1 15. A computer-readable medium having stored thereon an object  
2 attached to a kernel object, the object comprising:  
3 a first data entry identifying at least one user;  
4 a second data entry identifying an operation capable of being performed on  
5 the kernel object by the user identified by the first data entry; and  
6 a third data entry indicating a right for the user identified by the first data  
7 entry to perform the operation identified by the second data entry.

1           16.    A computer-readable medium according to Claim 15, wherein the  
2 kernel object is a transaction object, and the identified operation includes at least one of:  
3           set information regarding the transaction object,  
4           enlist the transaction object in the transaction,  
5           render data updates in connection with the transaction object durable,  
6           abort the operation on the transaction object,  
7           transmit data from the transaction object to another object,  
8           save the current point of the transaction at the transaction object, and  
9           transmit data regarding the transaction to another device.

1           17.    A computer-readable medium according to Claim 15, wherein the  
2 kernel object is a resource manager object, and the identified operation includes at least  
3 one of:  
4           retrieve information regarding the resource manager object,  
5           set information regarding the resource manager object,  
6           determine the state of a transaction at a moment of transaction failure,  
7           enlist the resource manager object in a transaction,  
8           register the resource manager object in the transaction,  
9           receive notification upon resolution of a transaction at the resource manager  
10 object, and  
11           set resource data in accordance with the transaction resolution.

1           18. A computer-readable medium according to Claim 15, wherein the  
2 kernel object is an enlistment object, and the identified operation includes at least one of:  
3           get information regarding the enlistment object,  
4           set information regarding the enlistment object,  
5           determine a state of enlistments at a moment of transaction failure,  
6           obtain and reference an enlistment key,  
7           rollback the transaction and to respond to notifications, and  
8           perform operations a superior transaction manager would perform.

1           19. A transaction method, comprising:  
2           implementing a transaction among kernel objects; and  
3           securing the transaction utilizing The Microsoft® Windows® operating  
4 system security model.

1           20. A transaction method according to Claim 19, wherein The  
2 Microsoft® Windows® operating system security model includes applying a security  
3 descriptor to at least one of the kernel objects participating in the transaction, and  
4 wherein the security descriptor identifies at least one user, an operation to be performed  
5 on the at least one kernel object to which the security descriptor is applied, and a right  
6 indicating that the identified user is permitted or prohibited to perform the operation.

1           21.    A method of implementing a transaction, comprising:  
2           attaching a security descriptor to at least one of plural objects utilized in a  
3 transaction; and  
4           performing an operation for a transaction on the at least one object in  
5 accordance with the rights accorded by the security descriptor attached to the at least one  
6 object.

1           22.    A method according to Claim 21, wherein the security descriptor  
2 includes identification for at least one user, an operation to be performed on the at least  
3 one object to which the security descriptor is attached, and a right indicating that the  
4 identified user is permitted or prohibited to perform the operation.

1           23.    A method according to Claim 22, wherein the at least one object is a  
2 transaction object.

1           24.    A method according to Claim 22, wherein the at least one object is a  
2 resource manager object.

1           25.    A method according to Claim 22, wherein the at least one object is  
2 an enlistment object.

1           26.    A method according to Claim 23, wherein the operation identified by  
2 the security descriptor attached to the transaction object includes at least one of:  
3           set information regarding the transaction object,



4 enlist the transaction object in the transaction,  
5 render data updates in connection with the transaction object durable,  
6 abort the operation on the transaction object,  
7 transmit data from the transaction object to another object,  
8 save the current point of the transaction at the transaction object, and  
9 transmit data regarding the transaction to another device.

1 27. A method according to Claim 24, wherein the operation identified by  
2 the security descriptor attached to the resource manager object includes at least one of:

3 retrieve information regarding the resource manager object,  
4 set information regarding the resource manager object,  
5 determine the state of a transaction at a moment of transaction failure,  
6 enlist the resource manager object in a transaction,  
7 register the resource manager object in the transaction,  
8 receive notification upon resolution of a transaction at the resource manager  
9 object, and  
10 set resource data in accordance with the transaction resolution.

1 28. A method according to Claim 25, wherein the operation identified by  
2 the security descriptor includes at least one of:

3 get information regarding the enlistment object,  
4 set information regarding the enlistment object,  
5 determine a state of enlistments at a moment of transaction failure,  
6 obtain and reference an enlistment key,

rollback the transaction and to respond to notifications, and  
perform operations a superior transaction manager would perform.

29. A kernel-level transaction system, comprising:  
means for implementing a transaction among kernel objects; and  
means for securing the transaction by applying a security descriptor to at  
least one of the kernel objects,  
wherein the security descriptor identifies at least one user, an operation to  
be performed on the kernel object to which the security descriptor is applied, and a right  
indicating that the identified user is permitted or prohibited to perform the operation.

30. A system according to Claim 29, wherein the kernel objects include:  
a transaction object to represent a transaction;  
a resource manager object to represent a resource participating in the  
transaction; and  
an enlistment object to enlist participants in the transaction.

31. A system according to Claim 30, wherein the security descriptor is  
applied to the transaction object, and the operation identified by the security descriptor  
includes at least one of:  
set information regarding the transaction object,  
enlist the transaction object in the transaction,  
render data updates in connection with the transaction object durable,  
abort the operation on the transaction object,

8 transmit data from the transaction object to another object,  
9 save the current point of the transaction at the transaction object, and  
10 transmit data regarding the transaction to another device.

1 32. A system according to Claim 30, wherein the security descriptor is  
2 applied to the resource manager object, and the operation identified by the security  
3 descriptor includes at least one of:  
4 retrieve information regarding the resource manager object,  
5 set information regarding the resource manager object,  
6 determine the state of a transaction at a moment of transaction failure,  
7 enlist the resource manager object in a transaction,  
8 register the resource manager object in the transaction,  
9 receive notification upon resolution of a transaction at the resource manager  
10 object, and  
11 set resource data in accordance with the transaction resolution.

1 33. A system according to Claim 30, wherein the security descriptor is  
2 applied to the enlistment object, and the operation identified by the security descriptor  
3 includes at least one of:  
4 get information regarding the enlistment object,  
5 set information regarding the enlistment object, and  
6 determine a state of enlistments at a moment of transaction failure.